10/594510

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL04/001191

International filing date: 30 December 2004 (30.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/534,190
Filing date: 02 January 2004 (02.01.2004)

Date of receipt at the International Bureau: 01 February 2005 (01.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/IL2004/001191
23 JAN 2005

PA 1268633

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

January 06, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/534,190*
FILING DATE: *January 02, 2004*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

G. Montgomery

W. MONTGOMERY
Certifying Officer

PTO/SB/16 (10-01)
Approved for use through 10/31/2002/ OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No.

INVENTOR (S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)
Moshe	Basel	10 Hapaamonim St, Raanana 43391, Israel
David	Allouch	5 Hatzill St., Raanana 43396, Israel

☐ *Additional inventors are being named on the_____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

A System and a Method for Authorizing Processes Operations on Internet Servers

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer number [ ] → *Place Customer Number Bar Code Label here*

Type customer number here

OR

☒ Firm or Individual Name	Appelfeld – Zer Law Office				
Address	29 Lilinblum st.				
Address					
City	Tel-Aviv	State		ZIP	66139
Country	Israel	Telephone	+972 3 516 3982	Fax	+972 3 516 2927

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒	Specification	*Number of Pages*	6	☐ CD(S), Number	
☒	Drawing(s)	*Number of sheets*	2	☐ Other (specify)	
☐	Application Data Sheet. See 37 CFR 1.76				

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

		FILING FEE AMOUNT($)
☒	Applicant claims small entity status. See 37 CFR 1.27.	
☐	A check or money order is enclosed to cover the filing fees	
☐	The Commissioner is herby authorized to charge filing fees or credit any payment to Deposit Account Number: [ ]	
☒	Payment by credit card. Form PTO-2038 is attached.	$.80

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☐ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE Moshe

TYPED or PRINTED NAME MOSHE BASOL__DAVID ALLOUCH

TELEPHONE +972 3 516 3982

Date December 24, 2003

REGISTRATION NO. *(if appropriate)*

Docket Number: B/0026/0000

USE ONLY FOR FILING A PRVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a Provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to Complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case) Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETE FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

PTO/SB/16 (10-01)
Approved for use through 10/31/2002/ OMB 065-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

8126\018

USE ONLY FOR FILING A PRVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a Provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to Complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case/ Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETE FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

A System and a Method for Authorizing Processes Operations on Internet Servers

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to network security and in particular to a system and a method for authorizing Internet session activities on network servers.

Background Art

Prior art of providing security to servers, which are connected to the Internet and allow access to their resources, includes several techniques of preventing and restricting the access of unauthorized users. Such techniques include using firewalls, secure servers and demanding users to identify before granting them access. The main drawback of such security methods is that once the users gain access, even if it is a highly restricted one, complex multi server systems find it hard to track the users' activities on the servers and prevent the misuse of the servers' resources.

Executing the users' requests in multi server systems usually requires the initiation of many processes on the different servers. In such cases the applications may not obtain any information about the processes' owners since their processes are initiated by other servers and they communicate only with them. In such cases the processes may all be owned by a single user ID with low permissions. Such cases make tracking a single user's activity impossible and this becomes a major security loophole.

US Patent No. 6,199,113 addresses this problem by establishing a session key for the users on their entry into a secured server. The session key is established only for users

whose identity is authenticated by an authenticating process which includes comparing the received details of their identity as given by the browser and the system's database. This solution guarantees that only the sessions of authorized users may operate on the secured server and that users that manage to enter without permission cannot gain access to the servers' resources. This may be an effective solution for systems which what to ensure that their access restriction are enforced, but does not provide the needs of systems which do not operate under the secure system criteria and which are required to be open to all users.

There is therefore a need for a security system that suits the modes of operation of open complex systems such as systems operating in multi tier architecture and want to grant limited access to all users without allowing exploitation of their resources.

US Patent Application No. 20020174220 provides a partial solution to this problem. It restricts the number of processes that each user may initiate on the servers and thus ensures that the system's computing resources are not all captured by a single user. This may reduce opportunities for denial of service attacks on the security of a server node, but it does not examine the nature of the operations which are executed by the users.

In order to allow a system to supervise the activities of its users there is a need for a means for limiting the operations of the system's users by monitoring and filtering out unauthorized activities.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a new system and method for providing network security for online servers by tracking the users' activity on them and preventing the occurrences of unauthorized events. This invention implements an innovative security approach

which focuses on the web servers' environment and operates inside it. The preferred embodiment of the present invention functions at the operating system level of the servers, it validates that each process on the servers is in keeping with a set of rules and with the privileges of the users' requests. The system compares between the level and scope of permissions given to the requests of the users and the operation done by processes that relate to them on the different servers. Whenever incompatibilities or inconsistencies are found, the security system filters out the inappropriate process operations.

This method blocks both unauthorized access to resources and prevents the misuse of accessible resources. Unauthorized access may include, for instance, attempts of unlicensed users to operate within the system whilst misuse of resources may include attempts to alter database records by users with read-only permissions or to initiate actions which exploit the servers' resources. Preventing misuse by users is the most significant capacity of the present security system since prior art includes several well known solutions for preventing unauthorized users from gaining access into servers and networks, but once users enter it, it is much more difficult to monitor their activities and this issue remains the blind spot of most of the prevailing security strategies.

FIG 1 illustrates an example for environments in which the said security system may operate. The client 100 connects the system 120 via the internet 110. The system may be comprised of a single tier architecture 120a or of a multi tier architecture 120b. While in the single tier architecture all facilities 121a, 122a, 123a are run on a single server 120a, in multi tier systems 120b the system facilities are divided into several servers 121b,

122b, 123b which are interconnected via a local network 125 and cooperate in accomplishing tasks.

Client users 100 which connect to system 120 initiate action requests in the system 120 such as gaining access to files or retrieving information from database. To execute such actions the system 120 must create processes in its servers. Complex tasks may demand creating more then one process, especially if they are executed on a multi tier architecture.

FIG 2 illustrates the user identification process. Tracking the progress of each user is achieved using tools which are similar in nature to those used by load balancer techniques. Users may connect to the server 120 either by using a unique personalized user identifier such as a user login or by using browsing means that do not demand identification. Whenever a user login is used, the system can easily associates the identity of the users to the session IDs that their requests produce. But even when users enter the server without yielding personal details, their requests may be traced back to their browser through the request's header. Since the users' requests are usually sent sequentially, each request contains an individual header. As illustrated in FIG 2, the header of a request initiated by the client 100 contains a session ID 210 (the cookie which is attached to the header of each request). The security system identifies the session ID 210, and if for any reason a session ID 210 is not available, the security system creates a unique identifier for the session on the request's first appearance.

In addition, the security system tracks the unique TCP port ID 220 given to the request. The port ID 220 may be associated with the session ID 210 since they are both unique identifiers. This pairing allows the security system to identify which session

activates each of the processes 230 in system 120. In the case of multi tier systems, where every process may create additional processes in a tree hierarchy, using this method allows the security system to associate a session ID to each server task. In such cases the web server 121b may also transfer tasks to the other servers of the system 122b, 123b through the network 125. The initial process creates a connection via network 125 with servers 122b, 123b in order to transfer commands and arguments. It then waits for a result through the same connection. In this case, when tasks are transferred from one server to the next, the same procedure of correlating the session ID with the processes it creates through the socket connection is repeated. This allows the security system to trace back the session ID, and through it the identity of its user, for every process in the network.

A block diagram of the preferred embodiment of the present invention is illustrated in FIG 3. The security system 300 comprises three main modules. The first is a session request identification module 320, operating on the web server 121. The second is a central module 340 which collects the information about the different processes, socket connections, port numbers, and session IDs. The information is shared through agents installed on the different servers. The central module 340 operates according to a set of rules that take into account the collected information about the session ID and its history. These rules may be fully configured and managed by the administrator by using the security system's administrative tools from a remote management console. The third module is the process filter 330 which executed the commands given by the central module 340 and restricts the operation of processes that are found to be invalid.

What is claimed is:

1. a security system for preventing unauthorized processes operations within network server environment , said system comprised of:

- agent module installed on each protected server for monitoring communication sessions and processes activation;

- central control module for tracing successive session having the same source based on identifying session header data as revived from the agent module;

- authorization module for checking all processing activation requests for determining access authorization based on the identified sessions which are related to said processing activation requests in accordance to pre-defined rules;

- filtering module installed on each server for blocking unauthorized

B\26\0\12

Figure 1

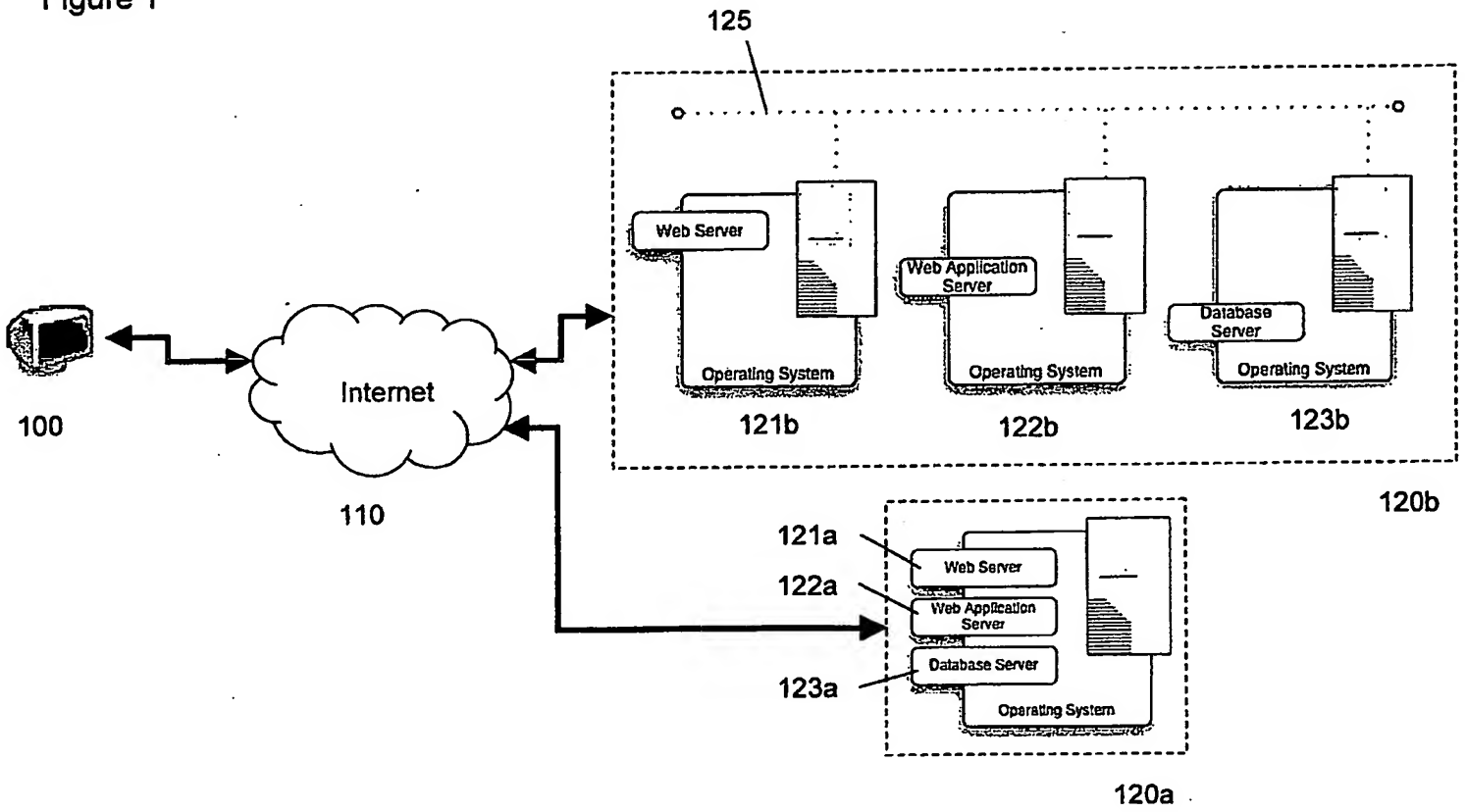

Figure 2

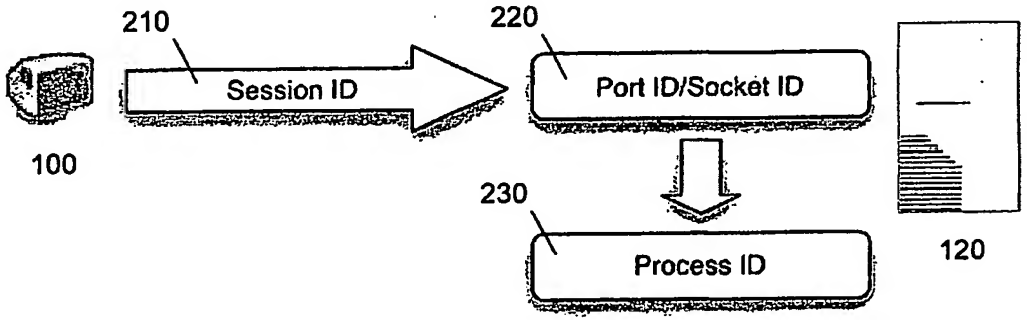

Figure 3